Safety & Mission Assurance News
Mission Success Starts With Safety
April 2000

SMA and Procurement – Partners for Safety and Success

-Frederick D. Gregory, Associate Administrator for Safety and Mission Assurance

NASA spends approximately 90 percent of its annual budget on acquisition of supplies and services. Unforeseen events in the acquisition cycle – like mishaps, contractor performance problems, funding shortfalls, schedule problems, or technological obstacles – can have serious and even catastrophic consequences. This is why the partnership between SMA and Procurement is so important.

Clear mission success requirements must be documented and used by all programs and projects. Whenever programs and projects are reviewed, we must make sure that there is a clear review of the capability for accomplishing the mission success requirements. SMA folks can participate in these reviews to make sure that the requirements are adequately defined. Procurement folks can make sure that procurement packages are not approved before the mission success criteria are established.

Safety goes hand in hand with mission success. Our contractors should have the same high standards for safety and health as we do. After all, this is where our money is being spent. One of the most obvious ways to do this is to implement the existing requirements we have established in the NASA FAR Supplement and the NASA Safety Manual. SMA and Procurement can work together to make sure we include the appropriate clauses related to safety into contracts, enforce requirements for safety and health plans, and have the proper SMA participation at the beginning of the contract development process. These three steps are key if we are to hold our contractors accountable for safety.

There has been great cooperation between SMA and Procurement. We need to continue work like the Risk-Based Acquisition Management (RBAM) initiative, which

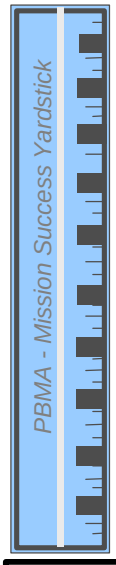
See "Procurement", p. 5

Process Based Mission Assurance Model *-J. Steven Newman*

Process Based Mission Assurance (PBMA) is the implementation of those management and systems engineering processes that are necessary to manage inherent program risks and maximize the likelihood of mission success…"Make it Safe, Make it Work, Manage Risk." PBMA assists the development of assurance requirements for new programs and the evaluation of assurance process implementation for ongoing programs OSMA's PBMA model is derived from best practices in aerospace, electronics, and automotive manufacturing, and reinforced by empirical evidence from NASA programs. The PBMA model provides a framework of high-level government expectations or "whats." Within those expectations, contractors have the flexibility to identify and implement their own process "hows."

The PBMA model is centered on ten key elements:

PBMA Elements



Management

Acquisition

Design & Engineering

Design Verification & Test

Software Design

Software Verification & Test

Manufacturing/Production

Manufacturing Verification & Test

Operations

Pre-Flight Verification & Test

How can it fail? Could someone get hurt? How likely would that be? Can we prevent that from happening? How can we implement controls? Let's get some outside review.

Each element reflects the themes of life-cycle risk management and defect/mishap prevention. For more, see:
http://www.hq.nasa.gov/office/codeq/qnews/pbm.pdf

NASA Administrator Meets with HEDS Assurance Board

-Bill Hill

Mr. Goldin met with the HEDS Assurance Board (HAB) on February 15, 2000, at Headquarters. He discussed his concerns relative to SMA; the following is a summary of what Mr. Goldin shared with the HAB.

Mr. Goldin indicated that SMA had good people, but they were not tough enough. NASA has had a number of safety issues surface. SMA is the key safety net for the Agency, but problems continue to poke through. Mr. Goldin believes that SMA needs to be mindful that they are separate from the Program. SMA should not have adversarial relationships with the Programs, but likewise SMA should not be too close to the Programs.

Mr. Goldin emphasized that NASA needs to do better on safety. We can't just talk safety, we have to live and breathe safety. SMA may be too close to the Programs to have the proper perspective. SMA needs to talk to the Programs, but not necessarily take everything at face value. Each SMA Director should do a self-assessment, consider the relationship with peers, subordinates, and Programs, and determine if he or she is clearly and appropriately focused. SMA Directors need to make sure they are working smart, not just hard. SMA Directors should all read and understand the Stephenson panel's Mars Climate Orbiter Mishap report. It shows the results of simple communications failures and a lack of understanding of how to do failure analysis. It shows the types of things that can happen if you don't have a sufficiently broad view to see the full picture. We need to take time each day to think about what we are doing from a strategic standpoint and to look over the horizon for what is coming. That is what leaders in this Agency need to do: spend more time considering what might be in the future. Mr. Goldin polled the room to find out how much time each SMA Director has blocked out on their calendar as free time to think each day. He urged the SMA Directors to keep enough time to think.

Mr. Goldin reinforced his position by discussing a Stephen Covey course he took, noting that 75% of senior management in this country (and the Agency) spend most of their time on tasks that are time critical, but very low in importance (we are all fire fighters.) We need to spend, as senior managers, more time focusing on tasks of high importance and low time criticality, such as strategic planning.

Mr. Goldin told the group that NASA could not afford to let catastrophic events occur in Human Space Flight. At JPL, we were lucky we were dealing with a spacecraft and not a human mission. SMA needs to have a stronger position and needs to maintain the proper perspective. JPL SMA had no idea about the problems with the Mars programs. To them, everything was proceeding just fine. NASA is very lucky we had this simple, English-Metric units error that caused us to step back and discover all the problems in the system. This error was a wake-up call that will help us get well. External teams have found problems with the Shuttle that SMA should have found. SMA should ask, "Why should we fly?" instead of "Why shouldn't we fly?"

Mr. Goldin stated that he wanted the Enterprise AA's to evaluate this year's programs and missions to see if there were any that may be likely to fail. HETE II is an example – the Program did not have enough money to do testing that would otherwise be the prudent thing to do, and chose to fly. Another example was that Kevin Kregel, the Shuttle Commander for the SRTM mission, asked why simulations were not being run in preparation for the mission. The answer was that the Program ran out of money. Mr. Goldin required the simulations to be done even if the mission was delayed.

Mr. Goldin told the group that the mission begins the day we have a concept. That is the day that SMA should start applying their knowledge and tools. SMA can't delegate their responsibilities to anyone else. SMA knows what needs to be done. SMA should determine how it is spending its time, how it is interfacing with Programs, and do a self-assessment to see what is needed to do the job right. SMA should be free to say anything…this is a judgement-free, blame-free assessment.

Mr. Goldin emphasized that the apparent lack of money is no excuse for not doing the right thing. It is better to not perform a mission if there is a lack of funding, than to pretend the funding exists or to cut corners that later result in increased risk to safety and mission success. Our managers need to make sure resources are available before proceeding. Mr. Goldin asked the HEDS Assurance Board to individually conduct a self-assessment of their activities and their relationships with the Programs and Projects. He asked that once SMA conducted its self-assessment he would come back and meet with them, noting that it should not be a year before this meeting is to take place, but should be held in one or two months.

NASA's Reliability and Maintainability Preferred Practices: A Safety & Mission Assurance Resource *-Wil Harkins*

In a recent Administrator's Weekly Health and Safety Topic, Mr. Goldin stressed the need for NASA to apply the lessons we've learned over the years to our current and upcoming programs. For many employees the natural follow up to Mr. Goldin's challenge was to ask, "Where can I find information on the lessons NASA has learned?" Part of the answer is NASA's Lessons Learned Information System (LLIS) at http://llis.nasa.gov. LLIS covers a variety of sources and a broad range of topics. However, LLIS is not the sole source of applied lessons within NASA. NASA Policy Directives, NASA Procedures and Guidelines Documents, and NASA-Standards are examples of requirements and guidance that have their roots in lessons learned.

From a reliability and maintainability perspective, two key resources that represent NASA's "best technical advice" are the "NASA Reliability Preferred Practices for Design and Test" (NASA Technical Memorandum 4322A) and "Recommended Techniques for Effective Maintainability" (NASA Technical Memorandum 4628). From the late 1980's to the late 1990's, Center representatives collected design and test practices that contributed to NASA mission success. NTM 4322A and NTM 4628 document these practices in a standard format. NTM 4322A includes information related to reliability practices associated with environmental conditions, design considerations, and analytical and test approaches for flight and ground support equipment. NTM 4628 provides similar information on maintainability practices. The two documents collectively contain approximately 200 practices that range from design considerations for selection of thick-film microelectronic circuits to the benefits of implementing maintainability on NASA programs.

Risk Management NPG in NODIS

Draft NPG 8705.X, "Risk Management Procedures and Guidelines," entered the NASA On-line Directives Information System (NODIS) on March 27 for 60 days review and comment by Headquarters Codes. Find NODIS at:
http://nodis.hq.nasa.gov/Nodis1.1/Welcome.html

Joint NASA Safety & Health Meeting *-Arthur Lee & Jonathan Mullin*

For the first time in more than 15 years, NASA Safety Managers and Occupational Health Program Managers met jointly to exchange ideas, discuss issues, and build synergy for NASA's efforts in safety and health. The February 29 - March 3 meeting was sponsored by OSMA and the Office of Life and Microgravity Sciences and Applications and hosted by the Kennedy Space Center (KSC). Representatives from all NASA Centers, the Jet Propulsion Laboratory, and the Office of Headquarters Operations attended. Representatives from the Architect of the Capitol were also present to benchmark NASA safety and health processes.

Mr. James Lloyd, Director, Safety and Risk Management Division, communicated the Administrator's expectations for the Agency Safety Initiative. Each Center described innovative ways of improving NASA workplace and operational safety and occupational health programs. The Ames Research Center and KSC reported that they will pursue Voluntary Protection Program certification this year (the Langley Research Center and the Johnson Space Center are already certified). A working group was established to recommend changes to make the Performance Evaluation Profile survey a more user friendly tool for evaluating and improving NASA safety programs.

KSC, Principal Center for Occupational Health, reviewed the Federal Worker 2000 Program and the Agency Return to Work Policy. KSC also gave a status of NASA's approaches to reduce injury and illness claims costs that are paid by the Department of Labor's Office Workers' Compensation Programs. OSMA reported that it is working with the Office of Procurement to include additional safety and health program guidance as part of Risk-Based Acquisition Management changes to the NASA FAR Supplement.

Participants agreed that NASA safety and occupational health programs have improved dramatically, but work remains to be done. OSMA distributed a list of common lessons learned from process verifications and the NASA Operations and Engineering Board reviews for participants to review for application at their Centers. OSMA committed to continue these reviews as a catalyst for improving NASA's safety posture.

The Safety Managers and Occupational Health Program Managers agreed to hold future joint meetings to continue team building and the beneficial exchange of programmatic information.

What is Probabilistic Risk Assessment? *-Dr. Michael Stamatelatos*

What is Probabilistic Risk Assessment?

Probabilistic Risk Assessment (PRA) is a systematic, comprehensive methodology to evaluate risks associated with every life-cycle aspect of complex engineered technological entities (facility, spacecraft, or power plant), including concept definition, design, construction and operation, and removal from service.

Risk is simply defined as a potential detrimental outcome of an activity or action (launch or operation of a spacecraft) that is subject to hazards. In a PRA, risk is characterized by two quantities: (1) the *magnitude* (or *severity*) of the adverse *consequences* that can potentially result from the given activity or action, and (2) the *likelihood* of occurrence of the given adverse consequences.

PRA usually answers three basic questions:

1. What can go wrong- what are the *initiating events*?
2. What and how severe are the potential detriments, or *consequences*?
3. How likely are the consequences, or what are their *probabilities* or *frequencies*?

To answer these questions, PRA uses Boolean logic (fault trees, event trees, event sequence diagrams, failure modes and effects analysis) and probabilistic and deterministic methods (thermal, fluid, structural or other engineering analyses) depending on the specific technology being analyzed.

What are the benefits of PRA?

PRA originated in the aerospace industry in the early 1960's. Other industries (nuclear power, chemical), US Government laboratories, and US Government agencies adopted and expanded PRA methods to higher levels of sophistication. Industry began using PRA reluctantly, at the request of some regulatory agencies, to answer safety concerns. After completing compulsory PRA efforts, organizations usually discovered benefits beyond compliance with regulation. These included new insights into, and an in-depth understanding of:

- Design flaws and cost-effective ways of eliminating them;
- Technical subtleties of complex systems and facilities, and new awareness even for the most experienced design and operating personnel;
- Design flaws and hardware-related, operator-related and institutional impacts on safety and cost-effective ways to implement upgrades;
- Approaches to reduce operation and maintenance costs while meeting or exceeding safety requirements;
- Technical bases for exemptions from unnecessarily conservative regulatory requirements.

PRA efforts have been successfully performed for complex technological entities at all phases of the life cycle, from concept definition and pre-design through safe removal from operation. Even for new or one-of-a-kind systems, where sparse supporting information is available, performing a PRA has proven to be an extremely valuable tool to cost-effectively improve safety design. For a more complete treatment of PRA, see http://www.hq.nasa.gov/office/codeq/qnews/pra.pdf

PRA Expert Joins OSMA

Dr. Michael Stamatelatos joined the NASA Headquarters Office of Safety and Mission Assurance as Manager of Risk Assessment on March 20, 2000. He will provide probabilistic risk assessment (PRA) awareness-level and practitioner-level training; consultation to Centers on the conduct of PRA; and leadership for developing the necessary infrastructure of PRA policy, procedures, guidelines, and tools.

Dr. Stamatelatos has 30 years experience in safety assessment and 20 years experience in performing and managing programs on probabilistic risk and reliability assessment for complex technological systems. He has taught PRA and quantitative reliability methods in the US, Russia, Ukraine, Romania, and Bulgaria. Dr. Stamatelatos received Ph.D., M.S., and B.S. degrees in Nuclear Science and Engineering from Columbia University. For the past nine years, he was Vice President of SCIENTECH, Inc., an international consulting engineering company where he developed and managed national and international safety, risk, and reliability assessment programs for the US Government and industry. Prior to that, he served as a Safety and Reliability Expert for the International Atomic Energy Agency (IAEA); as US representative to an IAEA panel on Probabilistic Risk Assessment (PRA); as a National Science Foundation (NSF) panel review expert for PRA methods; and as PRA Advisor to the Swiss Federal Research Institute.

"Procurement", from p. 1

will embed the principles of risk management into the acquisition regulations and the entire acquisition process. We need to keep working to integrate the elements of procurement, contract management, and safety and mission assurance, and implement a comprehensive program. High quality work done by the SMA and Procurement communities, shoulder to shoulder with the program/project personnel and up-front in a program's life cycle, will have a far-reaching impact on mission success.

Upcoming Events

- **15th Annual NASA Continual Improvement and Reinvention Conference**, April 26-27, Alexandria VA. Contact Geoff Templeton, (202) 358-2157, or see http://www.hq.nasa.gov/office/codeq/award.htm for more information.
- **Headquarters Safety Day**, May 4
- **Third Annual Assurance Technology Conference**, June 7-8, Glenn Research Center. Contact Frank Robinson on (216) 433-2340 for more information.

New OSMA Quality Assurance Manager

Tom Whitmeyer joined the Office of Safety and Mission Assurance (OSMA) on March 27, 2000, as Manager for the NASA Quality Assurance Program. Before coming to OSMA, Mr. Whitmeyer worked at the Goddard Space Flight Center in the Office of Flight Assurance. At Goddard he was responsible for providing assurance management of the EOS PM project. Mr. Whitmeyer previously provided quality assurance support to the Microwave Anisotropy Probe (MAP) project. Prior to his government service, Mr. Whitmeyer worked as a Safety and Mission Assurance engineer for 15 years performing a wide variety of safety, reliability, and quality assurance activities involving NASA, the DOD, and industry. Mr. Whitmeyer has a Bachelor of Science in Mechanical Engineering and a Masters of Science in Mechanical Engineering with an Astronautics concentration.

NASA Nondestructive Evaluation Working Group Continues 7th Year of Progress

-Ed Generazio

OSMA chartered the Nondestructive Evaluation Working Group (NNWG) in 1994 as an Agencywide forum for the integration of major nondestructive evaluation (NDE) program needs. This forum, managed by the Langley Research Center as lead Center (Ed Generazio, program manager), provides a focus for new technology initiatives, identification of NDE documentation requirements, new operating practices, and Center NDE infrastructure upgrades. OSMA funds NDE activities, and Center programs and projects provide approximately one-third co-funding.

During February 1-3, 2000, the NNWG representatives met at the Stennis Space Center for the 7th annual workshop. The NNWG reviewed FY 2001 NDE proposals and reported on accomplishments and advances. The Agencywide NDE Rapid Response Team (RRT), sponsored by the NNWG, continues to provide real-time assistance on mission-critical NDE issues. Recent use of the RRT has included:

- Shuttle orbiter window integrity verification after space debris impact and residual stress quantification,
- Characterization of damage to X-33 composites from thermal and pressure cycling,
- Astronaut space sickness research,
- Investigations of Peltier devices used on Hubble Space Telescope, and
- Establishment of defect standards for graphite epoxy components.

The RRT is available to any Center that requests NDE assistance.

Marshall Space Flight Center (MSFC) has developed NDE inspection techniques and procedures for assuring the integrity of friction stir welds (FSW) and FSW repairs on the Shuttle super-lightweight tank. MSFC's FSW NDE procedures have been successfully tested and adopted by Lockheed Martin at Huntsville and Michoud Assembly Facility in New Orleans. This development will result in large cost savings due to the reduction or elimination of scrapped components.

The Johnson Space Center is investigating advanced eddy current techniques to detect corrosion and moisture in hidden areas of the Orbiter structure. The goal is to detect corrosion on aluminum skins without removing thermal protection system tiles and blankets.

See "NDE", p. 6

"NDE", from p. 5

The Kennedy Space Center has successfully demonstrated a prototype valve health monitoring sensor system on ground support equipment valves. Partial opened or closed valves can be identified non-intrusively. A field system is being installed and tested on selected valves to gather input on the system's effectiveness and evaluate future potential applications.

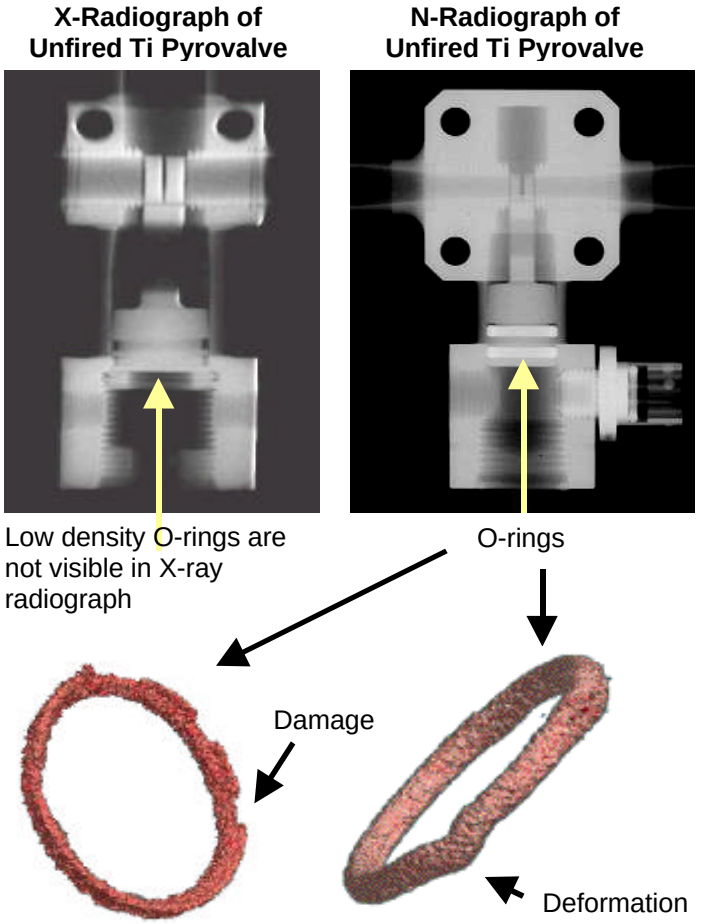
LaRC and Ames Research Center are jointly developing a device that non-invasively measures astronaut intra-cranial pressure, and are working to develop a flight-qualified unit for possible flight in 2002 that will help to understand space adaptation syndrome. This technology has been licensed to Kinetic Concepts, Inc., San Antonio, Texas, for use in head trauma patients.

Technology developments at other Centers include:

- Inspection technologies to assure the integrity of bonded assemblies of Shuttle, International Space Station, and Expendable Launch Vehicle components to help KSC accelerate ground processing time,
- Inspection technologies for characterizing thermal protective layers and composites,
- X-ray imaging as a process control tool for area array packaging of advanced electronic circuits,
- Neural-net holography for detecting blade damage and strain information in a rotating stage,
- Techniques for screening out materials with defects critical to X-ray detector performance, and
- NDE inspection techniques identified by White Sands Test Facility (WSTF) for assuring the integrity of installed pyrovalve seals (Figure 1).

The NNWG chair rotates yearly. Dr. Sam Russell, MSFC, served as chair during the past year. The new chair and vice-chair are Mr. Brad Parker, GSFC, and Dr. Carolyn Mercer, GRC, respectively. For more information see: http://nesb.larc.nasa.gov/nnwg71.html

Figure 1



Neutron-computed tomographs of O-rings deformed and damaged during installation in Ti-body pyrovalve

"Comparison of X-ray Imaging and Neutron Imaging of Pyrovalves with Installed O-rings (Regor L. Saulsberry/JSC-WSTF)"

Useful URLs

OSMA Home Page

http://www.hq.nasa.gov/office/codeq includes a wide variety of SMA information and links.

Site for On-Line Learning and Resources

Over 70 Web-based SMA training courses, as well as courses in Occupational Health, Procurement, Financial & Resources Management, IT Security, and Ethics. See http://solar.msfc.nasa.gov

Lessons Learned Information System

Knowledge that NASA has learned the hard way is at: http://llis.nasa.gov Make certain to enable Java on your browser.

NASA SMA Requirements

Hit the "Policy/Req" button on OSMA's home page, or go directly to:
http://www.hq.nasa.gov/office/codeq/doctree/doctree.htm

OSMA Newsletter

http://www.hq.nasa.gov/qnews has current and back issues. E-mail comments to: qnews@hq.nasa.gov

NASA Safety Reporting System

Confidential reporting of unresolved safety problems. See http://www.hq.nasa.gov/nsrs or contact the NSRS Project Manager at (703) 237-8083.